FIPS 140-2 and Common Criteria Compliant Operation for FortiOS™ 5.0.10

FIPS 140-2 and Common Criteria Compliant Operation for FortiOS™ 5.0.10

February 6, 2015

01-510-267768-20150206

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Contents

Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document discusses issues related to compliance, specifically Federal Information Processing Standards (FIPS) and Common Criteria (CC).

This chapter contains the following topics:

- Before you begin
- How this guide is organized

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How the guide is organized

This document contains the following sections:

FIPS and CC compliant operation describes how to install and use special FortiOS firmware builds certified to either Federal Information Processing Standards (FIPS) or Common Crideria (CC) requirements.

FIPS and CC compliant operation

Fortinet certifies specific FortiOS firmware builds that are compliant with U.S. Federal Information Processing Standards (FIPS), Common Criteria (CC) security requirements, or both.

This section describes how to install these certified builds on a FortiGate Next Generation Firewall and how to operate the unit in the FIPS-CC compliant mode. It provides information about features that differ from the standard firmware for your FortiGate unit.

At the publication date of this document, the latest FIPS and CC certified build is FortiOS 5.0 GA Patch 10 (b305).

This document is intended to be used by a system administrator.

This chapter contains the following sections:

Introduction to FIPS-CC

Security level summary

Fortinet performs Common Criteria certifications on specific FortiOS versions in combination with specific hardware models. Fortinet performs FIPS 140-2 certifications on specific FortiOS versions in combination with specific hardware models (FIPS 140-2 Level 2 certification) and on FortiOS independent of hardware (FIPS 140-2 Level 1 certification).

Documentation

The documentation for FortiGate units operated in FIPS-CC mode consists of this document and the standard FortiGate documentation set for the version of FortiOS that the FIPS-CC build is based on. This documentation is available from the Fortinet Technical Documentation web site at http://docs.fortinet.com.

Information on the Common Criteria certification is found in the Security Target. Information on FIPS 140-2 certification is found in the relevant Security Policy. These documents are available on the Fortinet Support web site from the same directory where you download the firmware.

Overview of Common Criteria compliant operation

Common Criteria compliant operation requires both that you use the FortiGate unit in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the FortiGate unit. You must ensure that:

- The FortiGate unit is installed in a secure physical location.
- Physical access to the FortiGate unit is restricted to authorized operators.
- Strong password policies are enabled by default.
- Administration of the FortiGate unit is permitted using only certified administrative methods. These are:
  - command line interface (CLI) access via the console connection
  - web-based manager via HTTPS

Within FIPS-CC mode, the FortiGate unit can be used in either of its two operation modes: NAT/Route or Transparent.

Use of non-FIPS-CC evaluated features

FIPS-CC mode does not prevent you from using features that were not part of the evaluated configuration. However, if you use these features, you may not be operating the FortiGate unit in strict compliance with the Security Target or Security Policy. Refer to the Security Target and relevant Security Policy for more information.

Effects of FIPS-CC mode

The following list describes, not necessarily in order, the effects of enabling FIPS-CC mode with respect to the default mode of operation.

Interfaces

- Immediately after switching to FIPS-CC mode, all network interfaces are down and have no IP address assigned. This includes virtual interfaces such as ssl.root. Configure interfaces as needed.
- By default, admin access (except for ping access) is disabled and must be enabled on a per-interface basis.
- Network interfaces, including virtual interfaces, cannot be configured for HTTP or Telnet administrative access.
- NPU support is disabled by default, but can be re-enabled.

Administration

- Administrative access via HTTPS requires strong cryptography: AES or 3DES encryption with SHA256 digest. DES encryption and MD5 digest are not available. SHA1 should not be used.
- By default, after three failed attempts to log on to an administrator account, the account is locked out for one hour. You can change the number of attempts permitted and the length of the lockout.
- Optionally, you can limit administrator access to scheduled times.
- On a CLI session, when an administrator logs out or the session times out, the FortiGate unit sends 300 carriage return characters to clear the screen. Note: if your terminal buffer is large, not all information from the session is cleared.
- The USB auto install options are disabled.
- The `get system status` CLI command display includes “FIPS-CC mode: enable”.
- When configuring passwords or keys, the FortiGate unit requires you to enter the password or key a second time as confirmation.
- The FortiGate unit performs self-tests at startup, when cryptographic keys are generated, and on a recurring basis. If any of these tests fail, the unit goes into FIPS Error mode and shuts down. The self-tests cannot be disabled, except by disabling FIPS-CC mode. Also, the administrator can run self-tests at any time. See “Running self-tests manually” on page 12.
- TFTP servers are insecure and are disabled by default. In non-FIPS-CC operation TFTP can be used to back up or restore the configuration remotely. In FIPS-CC mode, you should use a USB drive for this purpose. TFTP can be re-enabled using the `tftp` keyword in the `config system global` CLI command, but this is not FIPS-CC compliant operation.
- Remote access clients must meet security requirements. See “Remote access requirements” on page 13.
- USB auto-install options are disabled.
- The fnsysctl command, which provides some access to the underlying operating system, is not available.
- Virus attack reporting to FortiGuard Distribution Service (FDS) is disabled.

Routing

- Immediately after switching to FIPS-CC mode, no DNS addresses are configured.
- Immediately after switching to FIPS-CC mode, no default route is configured.

Logging

- Logging is enabled by default for:
  - new security policies
  - interfaces where administrative access is enabled
  - attempts to gain administration access on network interfaces where administrative access is not enabled
  - failed connection attempts to the FortiGate unit using TCP/IP ports other than 22 (ssh), 23 (telnet), 80 (HTTP), and 443 (HTTPS).
  - all configuration changes
  - configuration failures
  - remote IP lockout due to reaching maximum number of failed login attempts
  - log viewing
  - interface going up or down
  - other traffic: dropped ICMP packets, dropped invalid IP packets, session start and session deletion
- Logging is enabled for all event types at debug severity level.
- Memory logging is enabled on units that do not contain a hard disk. Logging includes traffic logging and all event types.
- Traffic logging to memory is available only in FIPS-CC mode.
- Reaching 95% of the local log storage capacity results in the FortiGate unit entering an error mode that shuts down all of the interfaces until the administrator intervenes. On units with only memory logging, the log space can fill quickly. To avoid triggering the error mode, you can set `diskfull` to `overwrite` for your local log device using the `config log memory setting` or `config log disk setting` CLI command.

Firewall

- Immediately after switching to FIPS-CC mode, all security policies are removed.
- Newly-created security policies have logging for allowed traffic enabled by default.
- Newly-created security policies are disabled and must be explicitly enabled.
- Blocking of spoofed TCP RST packets is enabled by default.

VPN

- The DES and MD5 algorithms are not available.
- Diffie-Hellman groups 1 through 5, and 14 through 18 are available to VPN configurations. Group 15 is the default. DH groups 15 through 18 use 3072 to 8192-bit keys. Fortinet recommends using group 15 or higher for FIPS-CC compliant VPNs between FortiGate units.

Initial configuration of the FortiGate unit

This section describes how to configure your FortiGate unit in the FIPS-CC mode of operation. Proceed as follows:

- Install the unit following the procedures in the documentation.
- Register your FortiGate unit with Fortinet.
- Download the FortiOS 5.0.10 firmware from Fortinet and install it on your unit.
- Verify the firmware version of your FortiGate unit.
- Enable FIPS-CC mode.

Installing the unit

Both the *Quick Start Guide* and the Getting Started section of the *Installation Guide* for your FortiGate unit provide instructions on the physical installation and initial configuration of your unit. When you have completed these procedures you will be able to access both the web-based manager and Command Line Interface (CLI).

Configuration of units with AMC/FMC modules

To use AMC/FMC modules, you must insert and configure them before enabling FIPS-CC mode. Modules inserted during FIPS-CC mode operation cause intermittent failures of integrity self-tests.

For more information about using AMC/FMC modules, refer to the documentation provided with your FortiGate unit.

Verifying the firmware version of the unit

Execute the following command from the command line:

```
get system status
```

The version line of the status display shows the FortiGate model number, firmware version, build number and date. For example:

```
Version: FortiGate-300C v5.0,build0305,141216 (GA Patch 10)
```

Verify in the relevant security target or security policy document that your firmware version, build number and date are correct.

Downloading and installing FIPS-CC firmware

To download the firmware

1. With your web browser, go to ftp://support.fortinet.com/ and log in using the name and password you received when you registered with Fortinet Support.
2. Navigate to the FortiOS 5.0.10 download page. Download the firmware build for your specific hardware model. Save the file on the management computer or on your network where it is accessible from the FortiGate unit.

Note that upgrading a FortiGate unit running a FortiOS 4.3 (or earlier) certified build in FIPS-CC mode to FortiOS 5.0.10 is not supported. Upgrading an existing FIPS-CC mode configuration is a manual process. Back up your configuration and contact Fortinet support before starting.

About the Fortinet entropy token

Generation of strong encryption keys requires a source of random numbers, sometimes referred to as entropy. A FortiGate unit can provide entropy, but a dedicated token provides better entropy. Based on a wide band, Gaussian white noise generator, the Fortinet entropy token provides users with a simple, FIPS 140-2 and NDPP CC validated source of entropy.

The Fortinet entropy token is compatible with FortiOS 5.0.10 or higher.

Installing the entropy token

Plug the entropy token into an available USB port on the FortiGate unit. Note that the entropy token requires a USB-A port.

Configuring the entropy token settings

Use of the entropy token is required in FIPS-CC mode. It is possible to disable the use of the token in FIPS-CC mode, but doing so means the unit will not be operating in a FIPS or CC compliant manner. There are three options for the entropy token setting:

- `enable` — token required (this is the default in FIPS-CC mode)
- `disable` — token is not required and is not used even if present
- `dynamic` — token is not required, but is used if present

The entropy token can also be used in the default, non-FIPS-CC mode of operation.

For example, to enable FIPS-CC mode with dynamic use of the entropy token enter:

```
config system fips-cc
  set entropy-token dynamic
  set status enable
end
```

Refer to "Enabling FIPS-CC mode", next for detailed information about enabling FIPS-CC mode.

Once the entropy token is enabled, it is used to seed the internal FortiOS Random Number Generator (RNG). The RNG is seeded during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes). The reseed interval is configured using a CLI command. In this example, the reseed interval is set to 720 minutes:

```
config system fips-cc
  set self-test-period 720
end
```

The self-test-period setting is only available in the FIPS-CC mode of operation.

The entropy token must be present to allow the RNG to seed or reseed from the token.

When FortiOS is configured in FIPS-CC mode with the entropy token enabled, if the token is not present at boot time or the reseed interval, the boot process will pause until the token is inserted. The following message is displayed on the console:

```
Please insert entropy-token to complete RNG seeding
```

The message is repeated until the token is inserted.

If the entropy token is set to dynamic and the token is not present at boot time or the scheduled reseed interval, the appliance will use the default, internal FortiOS seed method instead.

Enabling FIPS-CC mode

If you have verified the firmware version, you are ready to enable FIPS-CC mode.

When you enable FIPS-CC mode, all of the existing configuration is lost.

You must use a console connection to enable FIPS-CC mode. If you try to use another type of connection, a “check permission failed” error occurs.

The new password must be at least 8 characters long and must contain at least one each of:

- upper-case-letter
- lower-case-letter
- numeral
- non-alphanumeric character

To enable FIPS-CC mode

1. Plug the entropy token into a USB port on the FortiGate unit.
2. Log in to the CLI through the console port. Use the default admin account or another account with super_admin access profile. Enter the following commands:

```
config system fips-cc
  set status enable
end
```

If the FortiGate unit is currently in multi-VDOM mode, you need to precede the above commands with the command `config global`.

3. In response to the following prompt, enter the password for the administrator:

```
Please enter administrator password:
```

4. When prompted, re-enter the administrator password.

   The CLI displays the following message:

```
Warning: most configuration will be lost,
     do you want to continue? (y/n)
```

5. Enter `y`.

   The FortiGate unit restarts and runs in FIPS-CC mode.

Configuring interfaces

When FIPS-CC mode is initially enabled, all network interfaces including virtual interfaces are down and have no IP addresses assigned. You must use the console connection to peform the initial configuration of the unit. This example shows how to configure port1 with an IP address of 192.168.0.99 and administrative access to permit use of the web-based manager.

```
config system interface
  edit port1
    set ip 192.168.0.99 255.255.255.0
    set allowaccess https
    set status up
  end
```

For detailed information about configuring network interfaces, refer to the FortiGate documentation supplied with your unit.

Re-enabling NPU support

Support for NPU accelerated interfaces is disabled by default in FIPS-CC mode. The following CLI commands will re enable NPU support:

```
config system npu
  set dec-offload-antireplay enable
  set enc-offload-antireplay enable
  set offload-ipsec-host enable
end
```

FIPS-CC mode status indication

In FIPS-CC mode, the output of the `get system status` command includes

```
FIPS-CC mode: enable
```

Self-test settings

The default self-test period is every 1440 minutes. The following CLI command can change this to any period from 1 to 1440 minutes, inclusive.

```
config system fips-cc
  set self-test-period <minutes_int>
end
```

The self-test setting is also used as the reseed interval for the entropy token.

Running self-tests manually

The administrator can run self-tests manually at any time. To run all of the tests, enter the following CLI command:

```
execute fips kat all
```

To run an individual test, enter `execute fips kat <test_name>`. To see the list of valid test names, enter `execute fips kat ?`

Administration

When you invoke FIPS-CC mode for the first time, the FortiGate unit prompts you for a password to assign to the administrator account. After the initial configuration of administrators when you enable FIPS-CC mode, you can create additional administrator accounts as needed.

User guidance

It is the administrator's responsibility to ensure users know how to use the user authentication functions of the FortiGate unit, as described in the Authentication chapter of the FortiOS Handbook.

Remote access requirements

In FIPS-CC mode, remote administration is not allowed via HTTP, Telnet, or SSH, which are not secure. HTTPS or the console should be used.

Enabling administrative access

In FIPS-CC mode, the network interfaces by default do not allow administrative access, preventing you from using the web-based manager. You can re-enable use of the web-based manager using CLI commands on the console. This example adds HTTPS administrative access on the port1 interface to allow use of the web-based manager:

```
config system interface
  edit port1
    append allowaccess https
end
```

For detailed information about accessing the web-based manager, see “Connecting to the web-based manager“ in the *Installation Guide* for your unit.

Web browser requirements

To use the web-based manager in FIPS-CC mode, your web browser application must meet the following requirements:

- Authentication algorithm: PKCS1 RSA or DSS (in descending order of preference)
- Connection security: TLS 1.0

Configuration backup

Configuration backup files created in FIPS-CC mode are not compatible with backup files created in non-FIPS-CC mode. A FIPS-CC mode configuration backup cannot be restored in non-FIPS-CC mode and vice-versa.

You can create FIPS-CC configuration backup files to use for disaster recovery. They are valid on a replacement FortiGate unit or to restore configuration after you exit and then re-enter FIPS-CC mode.

For detailed information about creating configuration backup files, refer to the documentation provided with your FortiGate unit.

Configuration backup or restoration using TFTP is not permitted in FIPS-CC mode.

Firewall

FIPS-CC mode has additional requirements, settings and options compared to the default mode of operation.

Enabling Firewall policies

When you create a security policy in FIPS-CC mode, by default the policy is not enabled. You must explicitly enable it. In the web-based manager, after creating the policy, select the

checkbox at the beginning of the policy entry on the **Policy > Policy** page. In the CLI, enable a policy by setting its status to enable. You can do this when you create the policy or later:

```
config firewall policy
  edit 2
    set status enable
end
```

Required Firewall policies

Several firewall policies are required for CC compliance. Policies are required to:

1. Block local link traffic (address block 169.254.1.0 through 169.254.254.255)
2. Block Class E trafffic (240.0.0.0/4)
3. Restrict the IPv6 address space to the allocated global unicast space.

These policies are not created by default.

Blocking local link traffic

To block local link traffic, create a local link firewall address and then create policies for the interfaces you want to protect. The example below blocks local link source/destination traffic from the WAN to Internal interfaces:

```
config firewall address
  edit "Local-Link"
    set subnet 169.254.1.0 255.255.0.0
  end
config firewall policy
  edit 1
    set srcintf "wan"
    set dstintf "internal"
    set srcaddr "Local-Link"
    set dstaddr "all"
    set action deny
    set status enable
    set schedule "always"
    set service "ALL"
  next
  edit 2
    set srcintf "wan"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "Local-Link"
    set action deny
    set status enable
    set schedule "always"
    set service "ALL"
  next
end
```

Blocking Class E traffic

To block Class E traffic, create a Class E firewall address and then create policies for the interfaces you want to protect. The example below blocks Class E source/destination traffic from the WAN to Internal interfaces:

```
config firewall address
  edit "Class-E"
    set subnet 240.0.0.0 240.0.0.0
  end
config firewall policy
  edit 1
    set srcintf "internal"
    set dstintf "wan"
    set srcaddr "Class-E"
    set dstaddr "all"
    set action deny
    set status enable
    set schedule "always"
    set service "ALL"
  next
  edit 2
    set srcintf "wan"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "Class-E"
    set action deny
    set status enable
    set schedule "always"
    set service "ALL"
  next
end
```

Restrict the IPv6 address space to the allocated global unicast space

To restrict the IPv6 address space to the allocated global unicast space, create an IPv6 firewall address and then create policies for the interfaces you want to protect. The example below blocks global unicast source/destination traffic from the WAN to Internal interfaces:

```
config firewall address6
  edit "IPv6-Global-Unicast"
    set ip6 2000::/3
  next
end
config firewall policy6
  edit 1
    set srcintf "wan"
    set dstintf "internal"
    set srcaddr "IPv6-Global-Unicast"
    set dstaddr "all"
    set action deny
    set status enable
    set schedule "always"
    set service "ALL"
    set srcaddr-negate enable
  next
  edit 2
    set srcintf "wan"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "IPv6-Global-Unicast"
    set action deny
    set status enable
    set schedule "always"
    set service "ALL"
    set dstaddr-negate enable
  next
end
```

Note that this example covers the entire global unicast range and will block special ranges which could be legitimate, including all IPv6 Multicast (ff00::/8) as well as reserved addresses for 6to4 and ipv4-mapped addresses (::ffff:0:0/96, 64:ff9b::/96).

Firewall authentication

In FIPS-CC mode, user passwords must be 8 characters or more. FTP and Telnet mechanisms for Proxy User Authentication are not allowed, and SSL redirection must be enabled for the HTTP mechanism.

Additional settings

The following settings are required to maintain CC compliance:

```
config system global
  set anti-replay strict
  set check-protocol-header strict
  set check-reset-range strict
end

config system settings
  set ses-denied-traffic enable
  set strict-src-check enable
end
```

Logging

The Common Criteria protection profile requires logging of all traffic and logging of system events, including startup and shutdown of functional components. The severity threshold for logging is set to the lowest level: debug. This ensures that the maximum amount of information is logged.

Logging to external devices

Offloading logs to a remote server over a secure connection is required to maintain CC compliance. For information on how to offload logs to a FortiAnalyzer device over SSL, see the Logging and Reporting chapter of the FortiOS Handbook.

If the SSL connection with the FortiAnalyzer is interrupted, one (or both) of the following log messages will be displayed:

```
SSL write to <ip address> has failed.
SSL connection to <ip address> is successfully closed.
```

Please re-establish the SSL connection between the devices to maintain CC compliance.

Local logging

Logs are written to the FortiGate unit hard disk if the unit contains one. Models that do not contain a hard disk log to system memory.

The FortiGate unit generates warning log entries when the space allocated for the local logs reaches 75%, then 90% and finally 95% of capacity. When the local logs exceed 95% of capacity, the default action is to block further traffic and switch to Error mode. See “CC Error mode” on page 18 for more information. To prevent traffic blocking due to full log space, configure the FortiGate unit to overwrite the oldest log entries instead.

For memory logging, enter:

```
config log memory setting
  set diskfull overwite
end
```

For disk logging, enter:

```
config log disk setting
  set diskfull overwite
end
```

Logging settings

The following log settings must be enabled to maintain CC compliance:

```
config log setting
  set local-in-deny enable
  set loglocaldeny enable
end
```

Error modes

There are two error modes in FIPS-CC mode: FIPS Error and CC Error.

FIPS Error mode

When one or more of the self-tests fail, the FortiGate unit switches to FIPS Error mode. The FortiGate unit shuts down all interfaces including the console and blocks traffic.

To resume normal FIPS-CC mode operation, power cycle the unit. If the self-tests pass after the reboot, the unit will resume normal FIPS-CC operation. If a self-test continues to fail after rebooting, there is likely a serious firmware or hardware problem and the unit should be removed from the network until the problem is solved.

If the self-test failure persists across reboots, you can attempt to reload the firmware after formatting the units flash memory (via the boot menu). If the self-test failure persists after reloading the firmware and re-enabling the FIPS-CC mode of operation, contact Fortinet technical support.

CC Error mode

When current logs and rolled log files consume more than 95% of local log capacity, the FortiGate unit switches to CC Error mode, shuts down network interfaces and blocks traffic.

The FortiGate unit indicates Error mode as follows:

- The console displays “FIPS-CC-ERR”.
- “CC-ERR” is prepended to the console prompt, `CC-ERR FortiGate-300C$`, for example.

To resume normal FIPS-CC mode operation, you first must reduce the local logs to less than 95% of device capacity and exit error mode using the console connection.

To reduce logs

From the console, do any of the following:

- Delete selected logs using the `execute log delete` command. For more information, see the *FortiGate CLI Reference*. Ideally, you should reduce logs to 50% or less of device capacity.
- Delete all current log entries using the command `execute log delete-all`.

To exit CC Error mode

From the console, enter the following CLI command:

```
execute error-mode exit
```

The FortiGate unit resumes normal FIPS-CC operation unless there is still too little free space on the log device.

Disabling FIPS-CC mode

The only way that you can return the FortiGate unit to the normal mode of operation is to restore the factory default configuration. Enter the following CLI command:

```
execute factoryreset
```

Disabling FIPS-CC mode erases the current configuration, including VPN certificates and encryption keys for SSH and HTTPS.